

## CLAIMS

1           1.       Method for configuring a firewall (1) in a computer system (2) comprising  
2 objects (3), the objects (3) for which an access control policy is established being called  
3 resources (4), characterized in that it groups the objects (3) of the system into protection  
4 domains (5, 6), each firewall (1) ensuring the protection of an internal domain (5) relative to  
5 an external domain (6), and applies to the firewall in question a rule for controlling access  
6 between a source resource (4) and a destination resource only if said source and destination  
7 resources belong to the same protection domain (5) or (6).

1           2.       Method according to claim 1, characterized in that it determines the protection  
2 domain of the resources (4) by means of the network interfaces (10) of the firewall in  
3 question, interfaces through which the communications pass in order to reach said resources.

1           3.       Method according to claim 2, characterized in that it defines the zones (8)  
2 comprising networks or subnetworks, in that it associates the network interfaces (10) of the  
3 firewalls to which said zones are connected with an internal or external domain, in that it  
4 determines the incoming and outgoing network interfaces (10) of the current traffic, in that it  
5 analyzes whether said network interfaces are attached to an internal or external domain, and  
6 in that it applies the rule only if both network interfaces are attached to the same internal  
7 domain (5), which corresponds to the fact that the resources belong to the same protection  
8 domain.

1           4.       Method according to any of claims 1 through 3, characterized in that it  
2 composes groups of objects (3) for which the access control policy is identical and applies the  
3 rule between each of the resources of a source group and a destination group.

1           5.       Method according to any of claims 1 through 4, characterized in that it  
2 characterizes the rule with a local or global scope, in that it applies the rule to the resources in  
3 question only if said resources belong to the same protection domain (5) or (6) when the  
4 scope of the rule is local, and in that it applies the rule to all of the resources in question when  
5 the scope of the rule is global.

1 6. Device for implementing the method according to any of claims 1 through 5.

1 7. Device for configuring a firewall (1) in a computer system (2) comprising  
2 objects (3), the objects (3) for which an access control policy is established being called  
3 resources (4), characterized in that it comprises a central configuration machine (14) that  
4 makes it possible to group the objects (3) of the system into protection domains, each firewall  
5 (1) ensuring the protection of an internal domain (5) relative to an external domain (6), and to  
6 apply to the firewall in question a rule for controlling access between a source resource (4)  
7 and a destination resource only if said source and destination resources belong to the same  
8 protection domain (5) or (6).

1 8. Device according to claim 7, characterized in that it comprises a graphical  
2 interface (15) from which an administrator (7) can enter the protection domains (5) and (6)  
3 and the access control roles.

1 9. Device according to either of claims 7 and 8, characterized in that the  
2 graphical interface allows the administrator (7) to define a local or global scope for the access  
3 control rule, and in that the machine (14) applies the rule to the resources in question only if  
4 said resources belong to the same protection domain (5) or (6) when the scope of the rule is  
5 local, and applies the rule to all of the resources in question when the scope of the rule is  
6 global.

1 10. Software module for implementing the method according to any of claims 1  
2 through 5.

add B2  
1 #9130600-US3845/PB-T2147-906761